FOC - Solution to Exe 1

Yoni Zohar

December 15, 2011

1.a: Let $S \subseteq U$. We first show that $2SD\left(P,Q\right) \geq 2\left(P\left(S\right)-Q\left(S\right)\right)$. Since we show this for every $S \subseteq U$, this will imply that $SD\left(P,Q\right) \geq max_{S\subseteq U}\left(P\left(S\right)-Q\left(S\right)\right)$. Well: By definition, $2SD\left(P,Q\right)=\Sigma_{u\in U}\left|P\left(u\right)-Q\left(u\right)\right|$. By the triangular inequality, we get that:

$$\begin{aligned} & \Sigma_{u\in U}\left|P\left(u\right)-Q\left(u\right)\right| \\ = & \Sigma_{u\in S}\left|P\left(u\right)-Q\left(u\right)\right|+\Sigma_{u\in U\setminus S}\left|Q\left(u\right)-P\left(u\right)\right| \\ \geq & \left|\Sigma_{u\in S}\left(P\left(u\right)-Q\left(u\right)\right)\right|+\left|\Sigma_{u\in U\setminus S}\left(Q\left(u\right)-P\left(u\right)\right)\right| \end{aligned}$$

By more simple arithmetic manipulations, we get:

$$\begin{aligned} & \left|\Sigma_{u\in S}\left(P\left(u\right)-Q\left(u\right)\right)\right|+\left|\Sigma_{u\in U\setminus S}\left(Q\left(u\right)-P\left(u\right)\right)\right| \\ = & \left|\Sigma_{u\in S}P\left(u\right)-\Sigma_{u\in S}Q\left(u\right)\right|+\left|\Sigma_{u\in U\setminus S}Q\left(u\right)-\Sigma_{u\in U\setminus S}P\left(u\right)\right| \\ = & \left|P\left(S\right)-Q\left(S\right)\right|+\left|Q\left(U\setminus S\right)-P\left(U\setminus S\right)\right| \\ = & \left|P\left(S\right)-Q\left(S\right)\right|+\left|1-Q\left(S\right)-\left(1-P\left(S\right)\right)\right| \\ = & \left|P\left(S\right)-Q\left(S\right)\right|+\left|P\left(S\right)-Q\left(S\right)\right| \\ = & 2\left|P\left(S\right)-Q\left(S\right)\right| \\ \geq & 2\left(P\left(S\right)-Q\left(S\right)\right) \end{aligned}$$

In particular, $SD\left(P,Q\right) \geq max_{S\subseteq U}\left(P\left(S\right)-Q\left(S\right)\right)$. It is now enough to show that there exists S' such that the inequalities above turn into equalities. How come? Because it is always true that $max_{S\subseteq U}\left(P\left(S\right)-Q\left(S\right)\right) \geq P\left(S'\right)-Q\left(S'\right)$. If indeed $P\left(S'\right)-Q\left(S'\right)=SD\left(P,Q\right)$ (i.e. the inequalities turn into equalities), we get $max_{S\subseteq U}\left(P\left(S\right)-Q\left(S\right)\right) \geq P\left(S'\right)-Q\left(S'\right)=SD\left(P,Q\right)$, which gives us the other needed direction. I suggest $S' := \left\{u\in U \mid P\left(u\right)\geq Q\left(u\right)\right\}$. Trivially, for every $u \in S'$

$P(u) - Q(u) \geq 0$ and for every $u \notin S'$ $Q(u) - P(u) \geq 0$. Therefore, both" $\geq$ "s turn into $=$.

1.b: We show This by transitions from the left-hand side to the right-hand side. The non-trivial transitions (i.e. those that are not justified by definition, renaming, associativity of sum etc.) will be explained later.

$$\begin{aligned}
& SD\left(P^2, Q^2\right) \leq SD\left(P^2, (P,Q)\right) + SD\left((P,Q), Q^2\right) = \\
= \;& \Sigma_{u,v\in U}\left|P^2(u,v) - (P,Q)(u,v)\right| + \Sigma_{u,v\in U}\left|(P,Q)(u,v) - Q^2(u,v)\right| \\
= \;& \Sigma_{u,v\in U}\left|P(u)\cdot P(v) - P(u)\cdot Q(v)\right| + \Sigma_{u,v\in U}\left|P(u)\cdot Q(v) - Q(u)\cdot Q(v)\right| \\
= \;& \Sigma_{u,v\in U}\left|P(u)\cdot P(v) - P(u)\cdot Q(v)\right| + \Sigma_{v,u\in U}\left|P(v)\cdot Q(u) - Q(v)\cdot Q(u)\right| \\
= \;& \Sigma_{u,v\in U}\left(\left|P(u)\cdot P(v) - P(u)\cdot Q(v)\right| + \left|P(v)\cdot Q(u) - Q(v)\cdot Q(u)\right|\right) \\
= \;& \Sigma_{u,v\in U}\left(\left|P(u)\left(P(v) - Q(v)\right)\right| + \left|Q(u)\left(P(v) - Q(v)\right)\right|\right) \\
= \;& \Sigma_{u,v\in U}\left(P(u)\left|P(v) - Q(v)\right| + Q(u)\left|P(v) - Q(v)\right|\right) \\
= \;& \Sigma_{u,v\in U}\left(\left(P(u) + Q(u)\right)\left|P(v) - Q(v)\right|\right) \\
\leq \;& \Sigma_{u,v\in U} 2\cdot\left|P(v) - Q(v)\right| \\
= \;& 2\cdot SD(P,Q)
\end{aligned}$$

Justifications for non-trivial transitions:

1. The first inequality is due to Triangular Inequality,

2. The inequality before the last line is due to the fact that $P(u)$ and $Q(u)$ are probabilities, i.e. not greater than 1.

1.c: We need to show that for every PPT D, $\left|\Pr_{x\leftarrow Q_n}\left[D\left(1^n, x\right) = 1\right] - \Pr_{x\leftarrow Q_n}\left[D\left(1^n, x\right) = 1\right]\right| = neg(n)$. Let D be a PPT.

$$\begin{aligned}
\left|\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]-\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]\right| &= \\
\left|\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]-\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]\right. & \\
\left.+\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]-\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]\right| &\leq \\
\left|\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]-\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]\right| & \\
+\left|\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]-\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]\right| &
\end{aligned}$$

But we know that the latter equals $neg\left(n\right)+neg\left(n\right)=neg\left(n\right)$. Hence we have shown that $\left|\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]-\Pr_{x\leftarrow Q_n}\left[D\left(1^n,x\right)=1\right]\right|=neg\left(n\right)$ for every PPT D.

1.d: I propose the following ensembles over $[2n]$.

1. $Q_n\left(m\right)=\begin{cases}\frac{2^{-n}}{n} & EVEN\left(m\right)\\ \frac{1-2^{-n}}{n} & ODD\left(m\right)\end{cases}$
2. $P_n\left(m\right)=\begin{cases}\frac{1-2^{-n}}{n} & EVEN\left(m\right)\\ \frac{2^{-n}}{n} & ODD\left(m\right)\end{cases}$

For every n, P_n and Q_n are distributions over $[2n]$:

$$Q_n\left([2n]\right)=P_n\left([2n]\right)=n\cdot\frac{2^{-n}}{n}+n\cdot\frac{1-2^{-n}}{n}=1$$

In addition,

$$supp\left(Q_n\right)=supp\left(P_n\right)=[2n]$$

It is left to show that $SD(Q_n, P_n) = neg(n)$. Indeed,

$$
\begin{aligned}
& SD(Q_n, P_n) = \\
= \;& \frac{1}{2}\Sigma_{x\in[2n]}\left(\left|Q_n(x) - P_n(x)\right|\right) \\
= \;& \frac{1}{2}\Sigma_{x\in[2n]\cap EVEN}\left|Q_n(x) - P_n(x)\right| + \frac{1}{2}\Sigma_{x\in[2n]\cap ODD}\left|Q_n(x) - P_n(x)\right| \\
= \;& \frac{1}{2}n\cdot\left|\frac{2^{-n}}{n} - \frac{1-2^{-n}}{n}\right| + \frac{1}{2}n\cdot\left|\frac{1-2^{-n}}{n} - \frac{2^{-n}}{n}\right| \\
= \;& n\cdot\frac{1-2\cdot 2^{-n}}{n} \\
= \;& 1 - 2^{-n+1} \\
= \;& neg(n)
\end{aligned}
$$